7. Identify various vulnerabilities.

Types of Vulnerabilities in Cybersecurity

Vulnerabilities are weaknesses in software, hardware, or human processes that attackers can exploit to compromise security. Below are **the major types of vulnerabilities**, categorized by their impact and attack vector.

---

1. Software Vulnerabilities

- **Definition:** Flaws in software that allow unauthorized access, privilege escalation, or code execution.
- **Best for:** Understanding how software defects can be exploited.

Common Software Vulnerabilities:

- ✔ **Buffer Overflow** – Writing data beyond memory bounds, leading to code execution.
- ✔ **SQL Injection (SQLi)** – Injecting SQL queries via user input to access databases.
- ✔ **Cross-Site Scripting (XSS)** – Injecting malicious scripts into web pages.
- ✔ **Remote Code Execution (RCE)** – Running arbitrary code on a target system.
- ✔ **Insecure Deserialization** – Manipulating serialized objects to execute code.
- ✔ **Command Injection** – Executing system commands via user input.

Example:

- **CVE-2017-5638 (Apache Struts RCE)** – Allowed attackers to execute commands remotely due to improper input handling.

---

2. Network Vulnerabilities

- **Definition:** Weaknesses in network protocols, configurations, or devices.
- **Best for:** Understanding how attackers exploit misconfigured or vulnerable networks.

Common Network Vulnerabilities:

- ✔ **Unencrypted Traffic (No TLS/SSL)** – Data sent in plaintext can be intercepted.
- ✔ **Weak Authentication (Default Credentials, No MFA)** – Easy brute-force attacks.
- ✔ **Open Ports & Unpatched Services** – Attackers exploit outdated services.
- ✔ **Man-in-the-Middle (MITM) Attacks** – Intercepting network traffic.
- ✔ **ARP Spoofing** – Impersonating devices to intercept traffic.

Example:

- **CVE-2020-0601 (Windows CryptoAPI Spoofing)** – Allowed attackers to spoof TLS certificates.

3. Web Application Vulnerabilities

- **Definition:** Security flaws in websites and web applications.
- **Best for:** Understanding how web-based attacks work.

Common Web Vulnerabilities:

- **Cross-Site Request Forgery (CSRF)** – Trick users into performing unwanted actions.
- **Insecure Direct Object References (IDOR)** – Accessing unauthorized resources.
- **Server-Side Request Forgery (SSRF)** – Making internal requests from a vulnerable web server.
- **Clickjacking** – Tricking users into clicking hidden UI elements.
- **XML External Entity (XXE) Injection** – Exploiting XML parsers to read sensitive data.

Example:

- **CVE-2019-19781 (Citrix Netscaler SSRF)** – Allowed attackers to access internal services via SSRF.

---

4. Hardware & Firmware Vulnerabilities

- **Definition:** Security flaws in hardware components and embedded firmware.
- **Best for:** Understanding how physical and firmware-level exploits work.

Common Hardware Vulnerabilities:

- **Side-Channel Attacks (Spectre, Meltdown)** – Exploiting CPU behavior to leak data.
- **Backdoors in Firmware** – Hidden access left by manufacturers or hackers.
- **USB-Based Attacks (BadUSB, Rubber Ducky)** – Malicious USB devices executing commands.
- **BIOS/UEFI Vulnerabilities** – Attackers modifying firmware to persist malware.

Example:

- **CVE-2017-5715 (Spectre)** – A CPU vulnerability allowing attackers to access sensitive memory data.

---

5. Cryptographic Vulnerabilities

- **Definition:** Weaknesses in encryption algorithms or their implementation.
- **Best for:** Understanding how data encryption can be bypassed.

Common Cryptographic Vulnerabilities:

- **Weak Encryption (MD5, SHA1, DES)** – Can be cracked using brute-force or collision attacks.
- **Hardcoded Keys & Secrets** – Embedded passwords or cryptographic keys in software.
- **Padding Oracle Attacks** – Exploiting errors in encryption padding schemes.
- **Insecure Random Number Generators** – Weak randomness allows prediction.

Example:

- **CVE-2018-0495 (ROBOT Attack)** – Allowed decryption of TLS traffic due to RSA key vulnerabilities.

---

6. Human-Based (Social Engineering) Vulnerabilities

- **Definition:** Exploiting human error or manipulation to gain unauthorized access.
- **Best for:** Understanding how attackers use deception instead of technical exploits.

Common Human-Based Vulnerabilities:

- ✔ **Phishing Attacks** – Tricking users into revealing credentials via fake emails.
- ✔ **Spear Phishing** – Targeting specific individuals with personalized attacks.
- ✔ **Pretexting** – Impersonating a trusted entity to extract information.
- ✔ **Tailgating & Shoulder Surfing** – Physically accessing restricted areas or observing passwords.

Example:

- **Twitter Bitcoin Scam (2020)** – Attackers used social engineering to gain access to Twitter's internal tools and post fraudulent messages.

---

7. Misconfigurations & Weak Policies

- **Definition:** Security gaps due to improper system or application configurations.
- **Best for:** Understanding how poor settings create security risks.

Common Misconfigurations:

- ✔ **Exposed Admin Interfaces** – Leaving sensitive dashboards accessible to the public.
- ✔ **Excessive Permissions** – Users or processes have more access than needed.
- ✔ **Unrestricted CORS (Cross-Origin Resource Sharing)** – Allowing attackers to make unauthorized requests.
- ✔ **Default Credentials & Open Cloud Buckets** – AWS S3, Google Cloud Storage misconfigurations.

Example:

- **CVE-2021-22986 (F5 BIG-IP Misconfiguration)** – Allowed remote attackers to bypass authentication and execute commands.

---

8. Zero-Day Vulnerabilities

- **Definition:** Newly discovered vulnerabilities that have no official patch.
- **Best for:** Understanding emerging threats.

Common Zero-Day Risks:

- ✔ **No Available Patches** – Vendors have not released a fix yet.
- ✔ **Actively Exploited in the Wild** – Used in targeted attacks before disclosure.

✔ **Difficult to Detect** – Requires advanced monitoring and behavioral analysis.

Example:

- **CVE-2021-40444 (Microsoft Office Zero-Day RCE)** – Allowed attackers to execute malicious macros without user interaction.

---

9. Insider Threats & Supply Chain Vulnerabilities

- **Definition:** Security risks posed by internal employees, contractors, or third-party suppliers.
- **Best for:** Understanding threats beyond external hackers.

Common Insider & Supply Chain Risks:

✔ **Malicious Insiders** – Employees intentionally leaking or damaging data.
✔ **Compromised Software Updates** – Attackers inserting malware into legitimate updates.
✔ **Hardware Tampering** – Pre-installed backdoors in hardware components.

Example:

- **SolarWinds Supply Chain Attack (2020)** – Attackers compromised the software update process to distribute malware.

Conclusion

Understanding different types of vulnerabilities helps in identifying, preventing, and mitigating security risks.